UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/808,260	03/23/2004	Michael D. Brent	010327-008600US	4180

20350 7590 10/21/2008

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
BAYOU, YONAS A	

ART UNIT	PAPER NUMBER
2434	

MAIL DATE	DELIVERY MODE
10/21/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/808,260	Applicant(s) BRENT, MICHAEL D.	
	Examiner YONAS BAYOU	Art Unit 2434	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 August 2008*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6 and 8-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6 and 8-12* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03/23/2004* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This office action is in response to applicant's response filed on 08/21/2008.

2. Claims 1-6 and 8-21 are pending.

3. Claims 1 and 19-21 are amended.

4. Applicant's arguments have been fully considered but they are not persuasive.

5. When responding to the Office action, Applicant is advised to clearly point out the patentable novelty the claims present in view of the state of the art disclosed by the reference(s) cited or the objection made. A showing of how the amendments avoid such references or objections must also be present. See 37 C.F.R. 1.111(c).

Response to Arguments

1. Applicant, on page 6, last paragraph, of the remarks, argues Dotan fails to teach at least "comparing the stored representation of the configuration data obtained at the first time with a representation of the configuration data associated with the operating system for the computer system obtained at second time, wherein the operating system is actively operating at the second time" and that "the operating system continues to operate after the at least one remedial measure is performed."

Examiner respectfully disagrees and asserts that Dotan discloses executable programs comprise a series of instructions that are executed by a central processing unit (CPU) of a computer system containing the program, when the program is invoked.

The method of the present invention comprises comparing an initial state of an executable program to a final state of the program. If the final state of the program is different than the initial state, then the invented method generates an alarm signal to inform a user that the program most probably has been modified by a virus program and is now infected **[4:20-56 and figs. 2A-2B;** modified corresponding to deviation]. Particularly, when a computer user accesses an executable program for loading the program into memory from a storage medium, the invented method is invoked prior to the program being stored into memory. As the program is being loaded into memory, the method stores some pertinent information regarding the program, such as program length or header information, into memory to mark that state of the program as the initial state **[4:20-56 and figs. 2A-2B]**. After the initial state of the program is marked, execution of the program continues. When execution of the program is completed, the method again stores the program's pertinent information into memory, to mark that state of the program as the final state **[4:20-56 and figs. 2A-2B]**. Alternatively, after the initial state of the program is marked and the program is loaded into memory, at the moment when processing of the program commences, that state of the program is stored into memory as the final state of the program, as opposed to when processing of the program is completed **[4:20-56 and figs. 2A-2B]**. Once the final state of the program is marked and stored into memory, the method of the present invention compares the information indicating final state of the program with the information indicating the initial state of the program. If the final state of the program matches the initial state, then it is confirmed that the program was not modified and therefore not infected by a virus **[4:20-**

56 and figs. 2A-2B]. If it is determined that the final state of the program is different than the initial state, then the invented method generates an alarm signal to inform the user that the program has been modified by a virus and is now infected **[4:20-56 and figs. 2A-2B;** modified corresponding to deviation; alarm signal corresponding to remedy and the operating system inherently continue operating when storing and remedial measure/alarm signal are performed].

2. Examiner, however, in light of the above submission maintains the previous rejections while considering the amendments to the claims as follows:

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1-6 and 8-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dotan U.S. Patent Number 5,822,517 in views of Ostrovsky et al., Patent No.: 5,123,045.

Referring to claims 1, 19, 20 and 21, Dotan teaches a system, an article of manufacture and a method for detecting hostile software in a computer system comprising:

storing a representation of configuration data associated with an operating system for the computer system obtained at a first time **[column 4, lines 17-20]**;

comparing the stored representation of the configuration data obtained at the first time with a representation of the configuration data associated with the operating system for the computer system obtained at a second time, wherein the operating system is actively operating at second time **[column 4, lines 20-22 and figs. 2A-2B]**; and

if deviation is detected between the stored representation of the configuration data obtained at the first time and the representation of the configuration data obtained at the second time, automatically performing at least one remedial measure in response to the deviation detected, wherein the operating system continues to operate after the at least one remedial measure is performed **[column 4, lines 22-56 and figs. 2A-2B]**. Dotan does not appear to explicitly teach a method, wherein the stored representation of configuration data is encoded prior to being stored. However, Ostrovsky teaches that the contents held in the slots of the buffers 21 can be readily observed by adversaries. To prevent adversaries from gaining any useful knowledge from such observation, the contents of each slot are encrypted prior to being stored in such slots. It is preferred that a private key probabilistic encryption method is used, such as presented in S. Goldwasser and S. Micali, "Probabilistic Encryption", Journal of Computer and System

Science, Vol. 28, No. 2, 1984, 270-299. Whenever a value is stored in memory, every bit of the value is probabilistically encrypted. Specifically, a seed of the pseudo-random function F is stored into the protected CPU, and for every bit b, a new (unused before) argument i is picked. The encryption (i, b XOR (i)) is stored. Other encryption techniques, however, may be used **[col. 7, lines 1-15 and figs. 3-5]**. Dotan and Ostrovsky are analogous art because both teach software protection.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to modify the method of Dotan to include data is encoded prior to being stored of Ostrovsky because given that an adversary only sees encrypted contents, he is prevented from knowing the true contents of each slot, including the seeds. Hereinafter, it is assumed that all values stored in unprotected memory are already encrypted as described above, please see KSR International Co. v. Teleflex Inc., 550 U.S-, 82 USPQ2d 1385 (2007) for further interpretation.

Referring to claim 2, Dotan teaches a method for detecting hostile software in a computer system, wherein the configuration data relates to identification of executable code installed in the computer system **[column 4, lines 17-20]**.

Referring to claim 3, Dotan teaches a method for detecting hostile software in a computer system, wherein the configuration data relates to identification of a command line for invoking executable code associated with a particular file extension **[column 6, lines 4-9]**.

Referring to claim 4, Dotan teaches a method for detecting hostile software in a computer system, wherein the configuration data is obtained from a registry maintained by the operating system **[column 6, lines 1-7 and fig. 1]**.

Referring to claim 5, Dotan teaches a method for detecting hostile software in a computer system, wherein the configuration data obtained from at least one key associated with the registry **[column 6, lines 1-7]**.

Referring to claim 6, Dotan teaches a method for detecting hostile software in a computer system, wherein the configuration data is obtained from a file stored in the computer system **[column 6, lines 1-7]**.

Referring to claim 8, Dotan teaches a method for detecting hostile software in a computer system, wherein the configuration data is compared to a predefined value **[column 4, lines 65-66,** predefined value is corresponding to the state of the program].

Referring to claim 9, Dotan teaches a method for detecting hostile software in a computer system, wherein the configuration data is checked for addition of data **[column 6, lines 37-50, fig. 2A and fig. 2B]**.

Referring to claim 10, Dotan teaches a method for detecting hostile software in a computer system, wherein the configuration data is checked for removal of data **[column 4, lines 22-26,** an alarm signal inform a user that the data has been modified (addition/removal) see fig. 2A and 2B].

Referring to claim 11, Dotan teaches a method for detecting hostile software in a computer system, wherein the at least one remedial measure comprises determining a storage location associated with suspected executable code in the computer system **[column 4, lines 57-64]**.

Referring to claim 12, Dotan teaches a method for detecting hostile software in a computer system, wherein the at least one remedial measure comprises determining whether suspected executable code is currently executing **[column 4, lines 51-56]**.

Referring to claim 13, Dotan teaches a method for detecting hostile software in a computer system, wherein the at least one remedial measure further comprises terminating execution of the suspected executable code **[column 4, lines 57-64,** restoring the infected program occurs by terminating execution of the suspected program].

Referring to claim 14, Dotan teaches a method for detecting hostile software in a computer system, wherein the suspected executable code does not receive notification prior to being terminated **[column 4, lines 51-56,** prior to termination, the suspected executable program is being under the process of comparing initial state and final state].

Referring to claim 15, Dotan teaches a method for detecting hostile software in a computer system, wherein the at least one remedial measure comprises moving suspected executable code to a specified storage location for later evaluation **[column 4, lines 57-64]**.

Referring to claim 16, Dotan teaches a method for detecting hostile software in a computer system, wherein the at least one remedial measure comprises altering configuration data associated with the operating system to reflect the stored representation of the configuration data **[column 5, lines 8-14]**.

Referring to claim 17, Dotan teaches a method for detecting hostile software in a computer system, wherein the operating system is a Windows-based operating system **[column 6, lines 9-12]**.

Referring to claim 18, Dotan teaches a method for detecting hostile software in a computer system, wherein the operating system is a Linux-based operating system **[column 6, lines 9-12,** MS-DOS is corresponding to Linux-based operating system].

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to YONAS BAYOU whose telephone number is (571)272-7610. The examiner can normally be reached on m-f,7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571-272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Yonas Bayou/

Examiner, Art Unit 2434

10/15/08

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434